REMARKS

Claims 1-30 were pending in the patent application. By this amendment, Applicants add Claim 31. Authorization is hereby given to charge Deposit Account 50-0510 in the amount of $18.00 for the introduction of one new claim in excess of 20 total claims.

The Examiner has objected to the drawings due to the duplicate use of reference numeral 4. Applicants submit, herewith, a proposed drawing correction to Fig. 1 which corrects the error by changing the network to "14" and inserting table 4 in the terminal. An Amendment to the specification has also been submitted to change the description of the reference numeral from 4 to 14 on page 7. Applicants additionally submit new drawings sheets with Figs. 2-5 which include the Figure numbers. Finally, the drawings were objected to for failure to illustrate the subject matter of Claims 23 and 24, specifically the "partially output message." A proposed amendment to Fig. 5 is submitted herewith to address the objection. As further discussed below with reference to Claims 23 and 24, support for the amendment is found in the Specification at pages 20, 23 and 24. Applicants believe that the proposed drawing

SZ998-041   -23-

changes address the Examiner's concerns and request withdrawal of the objections to the drawings. Upon receipt of the Examiner's approval for the proposed drawing corrections, new drawings will be prepared and filed.

The Examiner has objected to the Specification for several informalities. By this amendment, Applicants submit amendments to each of the cited paragraphs to correct the informalities. Applicants respectfully request withdrawal of the objections.

The Examiner has rejected Claims 23 and 24 under 35 USC 112, concluding that the partially output message is not described in the Specification. Applicants respectfully disagree. Applicants direct the Examiner's attention to the description found on page 20, lines 19-21, and to the passage found from page 23, line 17 through page 24. The Specification clearly teaches, at page 20, lines 19-21 and at page 23, lines 17-18 that a "different component of the authentication vector" be displayed each time. In addition, the Specification teaches on page 24, lines 15-16 that "the authenticity output message (m_0) is communicated at least partially to the user". Applicants have submitted a proposed drawing correction to Fig. 5 to parallel the teachings. Applicants believe that the claim language is

SZ998-041   -24-

adequately supported by the Specification and respectfully request withdrawal of the 112 rejection.

The Examiner has rejected Claims 1, 3,4, 6, 7, 9-11, and 27-30 under 35 USC 102(b) as anticipated by the Merritt patent; Claim 2 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Daggar; Claims 5 and 8 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Giltner; Claims 12-19, 21-22, and 26 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Manduley; Claim 20 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Manduley further in view of Lessin; and Claim 25 under 35 USC 103 as unpatentable over the combined teachings of Merritt and Manduley and further in view of Daggar. For the reasons set forth below, Applicants respectfully assert that the claims, as amended, are patentable over the cited art.

The present invention teaches and claims a device, terminal, server, program storage device, and method for establishing trustworthy connections among a user, with or without a device inserted at a terminal, a terminal, and a server. Specifically, the user must know that the terminal is trusted by the server before the user will release any sensitive information to the terminal. Similarly, the

SZ998-041   -25-

server must know that the terminal seeking access to it is authentic. The server may also engage in an exchange to determine if the user, of a user device or of the terminal, is authorized to access the server. In all claimed embodiments of the invention, the server authenticates the terminal. Once the terminal has been authenticated, the server either communicates that information directly to the user by display at the user device, or communicates that information to the user by notifying the user device whereupon the user device causes the terminal to display the information to the user, when the user has a device that does not have display capabilities. Applicants respectfully assert that none of the cited prior art teaches or suggests a server communicating terminal authentication information directly to the user device. Applicants also assert that none of the prior art teaches or suggests that terminal authentication information be communicated to the user, whereupon the user or user device provides information to the terminal for the terminal to dynamically create a user-specific authenticity output message for display to the user. None of the cited art teaches or suggests that a terminal dynamically create an authenticity output message.

SZ998-041   -26-

The primary reference cited against the present application is the Merritt patent. The Merritt patent teaches a method for authenticating a terminal whereby a terminal contacts the server, the server provides a user-specific personal security phrase ("PSP") to the terminal and the terminal displays the PSP to the user. Under the Merritt method, the server does not communicate authentication information directly to a user device. Further, under the Merritt method, the terminal does not dynamically create an authenticity output message. Rather, the Merritt terminal outputs a server-generated message.

Applicants respectfully assert that the Merritt patent does not teach or suggest the invention as claimed. The claimed invention expressly recites that a terminal dynamically creates the authenticity output message after the server has authenticated the terminal (Claims 1, 4, 5, 6, 7, 8, 31). Furthermore, the pending claims expressly recite that the server provides terminal authentication information directly to the user device (Claims 2, 9-30). Still other claims expressly recite that the user device provides user-specific information to the terminal, after receiving terminal authentication information from the server, for use by the terminal in dynamically creating the

SZ998-041   -27-

authenticity output message (Claims 18, 29, and 31). Finally, Claim 3 expressly recites that a user device include a messaging component and a comparison component for verifying user-input authentication information, such that the device authenticates the user, whereas Merritt teaches that the terminal authenticates the user with a PIN.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Merritt patent does not teach a terminal which dynamically creates the authenticity output message after the server has authenticated the terminal, does not teach that the server provides terminal authentication information directly to the user device, does not teach that a user device provides user-specific information to the terminal for the terminal to dynamically create the authenticity output message, and does not teach that a user device authenticate a user, it cannot be maintained that the Merritt patent anticipates the invention as claimed.

Applicants further assert that the additionally cited patents do not provide the teachings which are missing from the Merritt patent. The Daggar patent is cited for teaching establishing card authenticity. However, Applicants

SZ998-041   -28-

respectfully assert that Daggar simply states that card authenticity must be established. Daggar neither teaches nor suggests that a user device have its own authentication component. Absent some teachings as to how Daggar would establish the authenticity of the card, it cannot be concluded that the claimed implementation is obviated. Rather, the combination of Merritt and Daggar would lead one to provide card authentication by the server, since the server is the only authenticating entity. Such clearly would not obviate the invention as claimed.

Similarly, Applicants assert that the Giltner patent does not provide the teachings which are missing from the Merritt patent. The Giltner patent is cited for teaching that reducing the amount of data to be transmitted will reduce transmission time. Accordingly, Giltner stores addressing codes. Storing addressing codes is not the same as storing authenticity output messages. Moreover, the claimed invention provides for storage of values in a lookup table for use in dynamically creating an authenticity output message. Since neither Merritt nor Giltner teaches or suggests dynamic generation of an authenticity output message, it cannot be concluded that storage of addressing information would obviate the invention as claimed.

SZ998-041   -29-

With respect to the Manduley patent, Applicants contend that the combination of Merritt and Manduley does not obviate the invention as claimed. The Examiner acknowledges that the Merritt patent does not teach or suggest providing a terminal authenticity message to the device. The Manduley patent has been cited for teaching a method for assuring that the user is actually in possession of the card. However, that is NOT what is being claimed. The invention as set forth in independent claim 12 expressly recites the server providing a terminal authenticity message to the device via the established second trusted connection. As claimed, the user device is being provided with confirmation that the terminal has been authenticated. User authentication is not being claimed. Moreover, sending terminal authentication information directly from a server to a user device, thereby eliminating the possibility of a terminal interfering with or falsely generating a terminal authentication message, is not taught or suggested by the Manduley user authentication.

Even if one were to combine the teachings of Merritt and Manduley, one would not arrive at the invention as claimed. The combination would produce a Merritt system wherein a user is first authenticated to the terminal, and

SZ998-041   -30-

then the terminal would proceed to seek its own authentication from the server for presentation, in the form of the PSP, to the user. Such would effectively teach away from the present invention since, by having the Manduley user authentication up front, the user would be forced to provide secure information to an untrusted terminal. Clearly such a combination does not teach or suggest the invention as claimed.

The addition of the Lessin patent teachings to the combination of Merritt and Manduley does not render the pending claims obvious. Lessin has been cited for teaching that a user enter a PIN. The combination of Merritt, Manduley and Lessin would again effectively teach away from the claimed invention since the user would be forced to enter his PIN at a terminal before establishing that the terminal was trusted. Clearly that does not obviate the language of Claim 20, which expressly states that the server first send terminal authentication information directly to the user, apart from the user device—and not the terminal—authenticating the user.

Similarly, the addition of Daggar to the combination of Merritt and Manduley would not obviate the invention as set forth in Claim 25. Daggar simply states that card

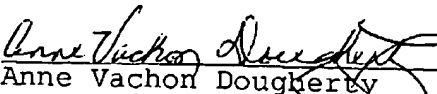SZ998-041   -31-

authenticity must be established. Daggar neither teaches nor suggests how Daggar would establish the authenticity of the card. Moreover, it cannot be concluded that the claimed implementation is obviated since the claim recites the limitations of Claim 12 further comprising authenticating the device to the server. Since none of the cited references teaches that the device be authenticated, that the server establish a trusted connection with the device and that the server communication terminal authentication information directly to the device along the trusted connection, it cannot be concluded that the combination obviate the claim.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

N. Asokan, et al

By: _Anne Vachon Dougherty_
Anne Vachon Dougherty
Registration No. 36,334
Tel. (914) 962-5910

SZ998-041   -32-